UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/664,992	09/18/2000	Teruyoshi Komuro	SONY-50L2204CON	5771

7590   03/29/2004

Wagner Murabito & Hao
Two North Market Street
Third Floor
San Jose, CA 95113

EXAMINER
TRUONG, THANHNGA B

ART UNIT	PAPER NUMBER
2135	

DATE MAILED: 03/29/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

PTO-90C (Rev. 10/03)

	Application No.	Applicant(s)
Office Action Summary	09/664,992	KOMURO ET AL.
	Examiner	Art Unit
	Thanhnga Truong	2135

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) FROM
THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed
  after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any
  earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on <u>18 September 2000</u>.

2a)☐ This action is **FINAL.**   2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is
closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) <u>1-20</u> is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) <u>1-20</u> is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on <u>18 September 2000</u> is/are: a)☒ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All   b)☐ Some * c)☐ None of:

      1.☐ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage
application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☒ Notice of References Cited (PTO-892)·

2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3)☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date <u>5</u>.

4)☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5)☐ Notice of Informal Patent Application (PTO-152)

6)☐ Other: _____.

U.S. Patent and Trademark Office

PTOL-326 (Rev. 1-04)   **Office Action Summary**   Part of Paper No./Mail Date 8

DETAILED ACTION

Double Patenting

1.   The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. See *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970);and, *In re Thorington,* 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent is shown to be commonly owned with this application. See 37 CFR 1.130(b).

Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

2.   Claims 1-20 are rejected under the judicially created doctrine of obviousness-type double patenting as being unpatentable over claims 1-16 of U.S. Patent No. 6, 223, 285. Although the conflicting claims are not identical, they are not patentably distinct from each other because the examined claims are either anticipated by, or would have been obvious over, the reference claims. Claims 1-20 of the application and claims 1-16 of U.S. Patent No. 6, 223, 285 are both directed to a method and system for transferring information using an encryption mode indicator (EMI). The claims differ in that claim 1 herein *does not* disclose a first decryption circuit for decrypting said data of said information packet in response to said extractor circuit indicating that said EMI code is of said first mode; and wherein said first encryption circuit, said second encryption circuit, said first decryption circuit and said second decryption circuit are coupled to receive a same cipher key. However, claims 3 and 7 which depend on claim 1 herein disclose the same limitations with claim 1 of U.S.

Patent No. 6, 223, 285. The claims also differ in that claim 8 herein fails to disclose a first and second hash circuits. However, claims 10 and 14 which depend on claim 8 herein disclose the same limitations with claim 1 of U.S. Patent No. 6, 223, 285. Therefore, it would have been obvious to modify the method of claims 1 and 8 of U.S. Patent No. 6, 223, 285 such that it would not disclose the first decrypting circuit and the first and second hash circuits. One having ordinary skill in the art would have been motivated to make such a modification to not include the first decryption circuit and the first and second hash circuit from claims 1 and 6 of U.S. Patent No. 6, 223, 285.

Drawings

3.   Figure 1 should be designated by a legend such as --Prior Art-- because only that which is old is illustrated. See MPEP § 608.02(g). A proposed drawing correction or corrected drawings are required in reply to the Office action to avoid abandonment of the application. The objection to the drawings will not be held in abeyance.

Specification

4.   The abstract of the disclosure is objected to because it exceeds the limitation of 150 words. Correction is required. See MPEP § 608.01(b).

Claim Rejections - 35 USC § 102

5.   The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless —

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

6.   Claims 1-3, 6-10, and 14-20 are rejected under 35 U.S.C. 102(e) as being anticipated by Park (US 6,028, 932).

     a.   *Referring to claim 1:*

i.   Park teaches:

(1)   a source device **[i.e., Figure 5 show the parallel data received at the interface portion and daisy chained down to the recording portion 8, this path is "a source device"]** for encoding an encryption mode identifier (EMI) code into an information packet and for transmitting said information packet over a communication interface, said source device comprising:

(a)   a first encryption circuit for encrypting data of said information packet provided said EMI code indicates a first mode; and a second encryption circuit for encrypting said data of said information packet provided said EMI code indicates a second mode **[i.e., referring to Figure 5, an encrypting portion 7 for encrypting the output of copy prevention information correcting portion 6, wherein the "a first encryption circuit" and "a second encryption circuit" are considered to include in the encrypting portion 7 (column 4, lines 4-6)]**; and

(2)   a sink device for receiving said information packet from said communication interface, said sink device comprising:

(a)   an extractor circuit for extracting said EMI code from said information packet **[i.e., As shown in FIG. 6, copy prevention information detecting portion 5 included a PES header detecting portion 10 for searching the parallel data in synchronization with a clock clk to detect the PES header, and a copy prevention information extractor 20, that is for "extracting said EMI code from said information packet", enabled by the PES header signal of PES header detecting portion 10 to detect the copy-prevention-information field (column 4, lines 8-14)]**; and

(b)   a second decryption circuit for decrypting said data of said information packet in response to said extractor circuit indicating that said EMI code is of said second mode **[i.e., referring to Figure 5, a decrypting portion 3 (in which "a second decryption circuit" is considered to include in this decrypting portion 3) for decrypting the output of key inserting portion 2 and transmitting it as parallel data (column 3, lines 62-64)]**; and

(3)   wherein said first mode is a copy prohibition mode indicating that said information packet is not to be reproduced by said sink device and wherein said second mode is a copy once inhibition mode indicating that said information packet is not to be reproduced more than once by said sink device **[i.e., First, when a mode of "No Copy" is detected from the additional copy information field of the PES header, VCR B is not able to enter its recording mode. Second, when a mode of "Copy Permitted" is detected in order to implement a copy prevention such as DAT mode, VCR B records but "No Copy" mode is recorded in the additional copy information field to interrupt recopying from a copying tape. This means that a secondary source tape may be formed from the original tape, the first source, but a third source tape cannot (column 5, lines 11-20)].**

      b.   *Referring to claim 2:*

        i.   Park further teaches:

(1)   wherein said sink device is a bit stream recording device and wherein said sink device further comprises a recording media for recording said information packet provided said EMI code is of said second mode and wherein said EMI code of said information packet is altered to said first mode by said sink device upon recording onto said recording media; **[i.e., there is provided a copy prevention apparatus for a digital video system including: a reproduction block for adding key information to a reproduced bit stream, and decrypting and transmitting it; and a recording block for searching key information of the bit stream transmitted from the reproduction block to extract copy prevention information, and encrypting and recording the bit stream according to the extracted copy prevention information. The reproduction block includes: reproduction means for reproducing data recorded on tape; key insertion means for adding key information to the bit stream of the reproduction means; and decryption means for decrypting the output of the key insertion means and transmitting it to a recording-side VCR (column 2, lines 60-67 through column 3, lines 1-6)].**

      c.   *Referring to claim3 :*

        i.   Park further teaches:

(1)   wherein said sink device further comprises a first decryption circuit for decrypting said data of said information packet in response to said extractor circuit indicating that said EMI code is of said first mode **[i.e., referring to Figure 5, a decrypting portion 3 (in which "a first decryption circuit" is considered to include in this decrypting portion 3) for decrypting the output of key inserting portion 2 and transmitting it as parallel data (column 3, lines 62-64)].**

     d.   *Referring to claim 6:*

         i.   Park further teaches:

         (1)   wherein said information packet represents a portion of a digital audio/visual program **[i.e., when recording is carried out by the satellite receiver or high-definition TV decoder and compressed video data is encoded in encoder 101, it is converted into a packet form in packet processing portion 102 as shown in Figure 1. If the compressed audio data is encoded in audio encoder 103, it is converted into a packet form in packet processing portion 104 (column 1, lines 55-60)].**

     e.   *Referring to claim 7:*

         i.   Park further teaches:

         (1)   wherein said first encryption circuit, said second encryption circuit, said first decryption circuit and said second decryption circuit are coupled to receive a same cipher key **[i.e., referring to key distribution when a conventional block-cipher or stream cipher algorithm such as data encryption standard (DES) encrypts or decrypts only with a secret key (column 2, lines 1-3)].**

     f.   *Referring to claims 8, 15, and 16:*

         i.   These claims have limitations that is similar to those of claim 1, thus they are rejected with the same rationale applied against claim 1 above.

     g.   *Referring to claims 9 and 17:*

         i.   These claims have limitations that is similar to those of claim 2, thus they are rejected with the same rationale applied against claim 2 above.

     h.   *Referring to claim 10:*

i.   This claim has limitations that is similar to those of claim 3, thus it is rejected with the same rationale applied against claim 3 above.

i.   *Referring to claim 14:*

i.   Park further teaches:

(1)   a first hash circuit for generating said first key based on a common key; and a second hash circuit for generating said second key based on said common key and wherein said common key is transferred between said sink device and said source device before said information packet is received by said sink device [i.e., **referring to Figure 3, "a first hash circuit" and "a second hash circuit" are considered to include in key supply portion 107**].

j.   *Referring to claim 18:*

i.   Park further teaches:

(1)   wherein said step of said source device receiving an information packet having a copy protection mode includes the step of said source device translating said information packet having encoded CCI information to extract said copy protection mode [i.e., **referring to FIG. 5, a copy prevention apparatus of the present invention comprises a reproducing portion 1 for reproducing data recorded on tape, a key inserting portion 2 for adding a tape header start code and key field at the front end of a bit stream of reproducing portion 1, a decrypting portion 3 for decrypting the output of key inserting portion 2 and transmitting it as parallel data, a key detecting/correcting portion 4 for detecting a key field from the parallel data transmitted from decrypting portion 3, a copy prevention information detecting portion 5 for detecting a PES header from the key field detected and extracting copy prevention information, a copy prevention information correcting portion 6 for correcting the output of copy prevention information detecting portion 5 if necessary, an encrypting portion 7 for encrypting the output of copy prevention information correcting portion 6, and a recording portion 8 for recording the output of encrypting portion 7 on tape (column 3, lines 58-67 through column 4, lines 1-8)**].

k.   *Referring to claim 19:*

i.   This claim has limitations that is similar to those of claim 6, thus it is rejected with the same rationale applied against claim 6 above.

I.   *Referring to claim 20:*

i.   This claim has limitations that is similar to those of claim 5, thus it is rejected with the same rationale applied against claim 5 above; and

ii.   Part further teaches:

(1)   wherein said sink device is a bit stream recorder [i.e., and recording means, that is "a bit stream recorder", for recording the bit stream encrypted in the encrypting means (column 3, lines 15-16)].

7.   Claims 1, 3-8, 10-13, 15-16, and 18 are rejected under 35 U.S.C. 102(e) as being anticipated by Yamauchi et al (US 6,047, 103).

a.   *Referring to claim 1:*

i.   Yamauchi teaches:

(1)   a source device **[i.e., the information processing apparatus shown in FIG. 15 includes a disk reproduction drive 125, that is "a source device", as the data transmitting device and an AV signal processor 126 as the data receiving device (column 25, lines 33-36)]** for encoding an encryption mode identifier (EMI) code into an information packet and for transmitting said information packet over a communication interface, said source device comprising:

(a)   a first encryption circuit for encrypting data of said information packet provided said EMI code indicates a first mode; and a second encryption-circuit-for encrypting said data of said information packet provided said EMI code indicates a second mode [i.e., referring to Figure 15, an encrypting section included in a disk reproduction drive 125, for converting the retrieved digital data into encrypted digital data, wherein the "a first encryption circuit" and "a second encryption circuit" are considered to include in this encrypting section (column 5, lines 60-61)]; and

(2)   a sink device **[i.e., the information processing apparatus shown in FIG. 15 includes a disk reproduction drive 125 as the data transmitting device and an AV signal processor 126 as the data receiving device ,**

that is "a sink device" (column 25, lines 33-36)] for receiving said information packet from said communication interface, said sink device comprising:

(a)   an extractor circuit for extracting said EMI code from said information packet **[i.e., referring to Figure 15, a controller 128, that is an extractor for "extracting said EMI code from said information packet" (column 25, lines 60-65)];** and

(b)   a second decryption circuit for decrypting said data of said information packet in response to said extractor circuit indicating that said EMI code is of said second mode **[i.e., referring to Figure 15, a decrypting section included in an AV signal processor 126 (in which "a second decryption circuit" is considered to include in this decrypting section) for converting the encrypted digital data into decrypted digital data (column 6, lines 51-52)];** and

(3)   wherein said first mode is a copy prohibition mode indicating that said information packet is not to be reproduced by said sink device and wherein said second mode is a copy once inhibition mode indicating that said information packet is not to be reproduced more than once by said sink device **[i.e., The CGMS code "00" indicates that the copying is permitted, "10" indicates that one-generation copying is permitted, and "11" indicates that copying is prohibited (column 13, lines 45-48)].**

        b.   *Referring to claim3 :*

           i.   Yamauchi further teaches:

                (1)   wherein said sink device further comprises a first decryption circuit for decrypting said data of said information packet in response to said extractor circuit indicating that said EMI code is of said first mode **[i.e., referring to Figure 15, a decrypting section included in an AV signal processor 126 (in which "a first decryption circuit" is considered to include in this decrypting section) for converting the encrypted digital data into decrypted digital data (column 6, lines 51-52)].**

        c.   *Referring to claim 4:*

           i.   Yamauchi further teaches:

(1)   wherein said communication interface is a serial communication interface conforming to the IEEE 1394 communication standard and wherein said information packet is a digital information packet **[i.e., As the digital interface, the SCSI was used in Examples 1 and 3 and the ATAPI was used in Example 2. Other interfaces may also be used as long as they can transmit AV digital data and connect a plurality of devices. For example, a digital interface defined in the IEEE P1394 may be used (column 42, lines 32-36)]**.

    d.   *Referring to claim 5:*

        i.   Yamauchi further teaches:

(1)   wherein said source device is a broadcast receiver device and further comprises a receiver circuit for receiving an information packet encoded with CCI information and for extracting a copy protection code therefrom and wherein said sink device is unable to process an information packet encoded with CCI information **[i.e., referring to Figure 15, a disk reproduction drive 125, that is "a source device" which is considered to be "a broadcast receiver device"]**.

    e.   *Referring to claim 6:*

        i.   Yamauchi further teaches:

(1)   wherein said information packet represents a portion of a digital audio/visual program **[i.e., the digital data received by the MPEG decoder 606 is subjected to a predetermined process and converted into a digital video signal and a digital audio signal. The digital video signal is output to the video signal processor 48. The digital audio signal is converted into an analog audio signal by the D/A conversion circuit 607 and audibly output via a speaker 47S (column 20, lines 3-9)]**.

    f.   *Referring to claim 7:*

        i.   Yamauchi further teaches:

(1)   wherein said first encryption circuit, said second encryption circuit, said first decryption circuit and said second decryption circuit are coupled to receive a same cipher key **[i.e., an encrypting function E(KEY1, DATA) encrypts data "DATA" with an encrypting key "KEY1". The encrypting function**

E(KEY1, DATA) has an inverse function, i.e., a decrypting function D(KEY2, DATA) where KEY2 denotes a decrypting key. That is, when EncryptData=E(KEY1, Data) where "EncryptData" denotes encrypted data, Data=D(KEY2, EncryptData) is satisfied. Accordingly, the original data "Data" can be obtained by operating the decrypting function D(KEY2, EncryptData) for the encrypted data "EncryptData" which has been encrypted by the encrypting function E(KEY1, Data). In this example, it is assumed that the encrypting key KEY1 in the encrypting function E is equal to the decrypting key KEY2 in the decrypting function D (i.e., "KEY1"="KEY2") (column 27, lines 34-46)].

   g. *Referring to claims 8, 15, and 16:*

    i. These claims have limitations that is similar to those of claim 1, thus they are rejected with the same rationale applied against claim 1 above.

   h. *Referring to claim 10:*

    i. This claim has limitations that is similar to those of claim 3, thus it is rejected with the same rationale applied against claim 4 above.

   i. *Referring to claim 11:*

    i. This claim has limitations that is similar to those of claim 4, thus it is rejected with the same rationale applied against claim 1 above.

   j. *Referring to claim 12:*

    i. This claim has limitations that is similar to those of claim 1, thus it is rejected with the same rationale applied against claim 1 above.

   k. *Referring to claim 13:*

    i. This claim has limitations that is similar to those of claim 6, thus it is rejected with the same rationale applied against claim 6 above.

   l. *Referring to claim 18:*

    i. Yamauchi further teaches:

     (1) wherein said step of said source device receiving an information packet having a copy protection mode includes the step of said source device translating said information packet having encoded CCI information to extract said copy protection mode [i.e., accordingly, in order to protect AV data at a high

security level, the information processing apparatus of Example 2 is provided with components which encrypt and decrypt data, in addition to the mutual authentication between the data transmitting device and the data receiving device. With this configuration, since AV data has been encrypted, the copyright protection of AV data is ensured even if AV data on the I/O bus 122 is extracted by the controller 128 due to an erroneous operation (column 25, lines 57-65)].

Conclusion

8.   The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

a.   Park (US 5, 761, 302) discloses a copy prevention method and apparatus for a digital video system is disclosed including the steps of: (a) adding a header area of a header start code and key field to a reproduced bit stream; (b) decrypting and transmitting the bit stream to which the header area is added; (c) detecting a key field of the decrypted and transmitted bit stream and detecting copy prevention information; and (d) encrypting the bit stream according to information detected form step (c) and recording it on tape (see abstract).

b.   Mionet et al (US 5, 920, 627) discloses an encryption device can be used to encrypt information units conveyed by cells that are broadcast from an optical broadcast node to network units by a passive optical network. Each cell conveys at least one information unit and each information unit is addressed to a respective subscriber terminal. The device includes an encryption system that receives in clear at least one key from at least one decryption device located in a network unit. Applications include ATM telecommunication networks (see abstract).

c.   Komuro et al (US 6, 223, 285) discloses a method and system for transferring information using an encryption mode indicator (EMI). The present invention provides several secure information communication modes in which data (e.g., representing an audio/visual work) can be transmitted from a source device to a sink device (receiving station) in a number of secure modes (see abstract).

d.   Kato et al (US 6, 618, 549) discloses an information processing apparatus comprises an extracting circuit for extracting main information including first

copy control information and auxiliary information representing attributes of the main information from input information; a first generating circuit for generating second copy control information based on the auxiliary information extracted by the extracting circuit; and an adding circuit for adding the second copy control information generated by the first generating circuit to the main information extracted by the extracting circuit (see abstract).
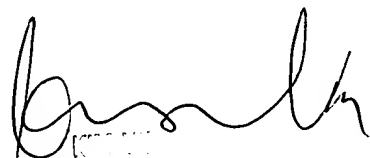
Any inquiry concerning this communication or earlier communications from the examiner should be directed to Thanhnga (Tanya) Truong whose telephone number is 703-305-0327.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 703-305-4393. The fax and phone numbers for the organization where this application or proceeding is assigned is 703-872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.

TBT

March 22, 2004